



DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Exámen final

09 de Diciembre del 2025

Fundamentos de Lenguajes para Computación Cuántica

Integrante	LU	Correo electrónico
Bagnasco Mugillo, Lautaro	1173/21	lbagnasco@dc.uba.ar
Laks, Joaquín	??	??
Vekselman, Natan	338/21	natanvek11@gmail.com
Romani, Rafael	775/21	rafaromani243@gmail.com



Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Ciudad Universitaria - (Pabellón 0/Planta Alta)

Intendente Güiraldes 2610 - C1428EGA

Ciudad Autónoma de Buenos Aires - Rep. Argentina

Tel/Fax: (++54 +11) 4576-3300

<http://www.exactas.uba.ar>

Parte I: Lógica, cálculo lambda, y el isomorfismo de Curry-Howard

Ejercicio 8: demostrar el siguiente lema

Lema 2.7

1. Si \rightarrow_R satisface la propiedad del diamante, entonces es Church-Rosser.
2. Si \rightarrow_R es Church-Rosser, entonces tiene formas normales únicas.

Lema 2.7.1

Sea \rightarrow_R que satisface la propiedad del diamante, es decir que, si $t \rightarrow_R r_1$ y $t \rightarrow_R r_2$ entonces existe un s tal que $r_1 \rightarrow_R s$ y $r_2 \rightarrow_R s$. Queremos ver que si $t \xrightarrow{R}^* r_1$ y $t \xrightarrow{R}^* r_2$ entonces existe un s tal que $r_1 \xrightarrow{R}^* s$ y $r_2 \xrightarrow{R}^* s$.

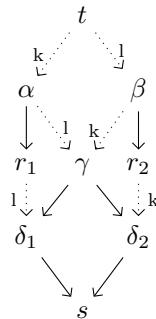
Sean t, r_1, r_2 tales que $t \xrightarrow{R}^* r_1, t \xrightarrow{R}^* r_2$. Si $t \xrightarrow{R}^* r_1$ existe una secuencia $\alpha_1, \alpha_2, \dots, \alpha_{k-1}$ tal que $t \rightarrow_R \alpha_1 \rightarrow_R \alpha_2 \rightarrow_R \dots \rightarrow_R \alpha_{k-1} \rightarrow_R r_1$, simétricamente para r_2 existe una secuencia $\beta_1, \dots, \beta_{l-1}$. Notamos esto $t \xrightarrow{R}^k r_1, t \xrightarrow{R}^l r_2$. Veamos por inducción en k y l que es Church-Rosser.

Para $l, r \leq 1$ se sostiene que es CR pues es la propiedad del diamante.

Veamos inductivamente que se sostiene para $l+1, r+1 \leq n+1$. **Hipótesis inductiva:** Si $t \xrightarrow{R}^k r_1, t \xrightarrow{R}^l r_2$ entonces existe un s tal que $r_1 \xrightarrow{R}^l s, r_2 \xrightarrow{R}^k s$.

Sean t, r_1, r_2 tales que $t \xrightarrow{R}^{k+1} r_1, t \xrightarrow{R}^{l+1} r_2$. Por definición de \xrightarrow{R}^{+1} existen α y β tales que $t \xrightarrow{R}^k \alpha \rightarrow_R r_1$ y $t \xrightarrow{R}^l \beta \rightarrow_R r_2$. Luego, por hipótesis inductiva tenemos que existe un γ tal que $\alpha \xrightarrow{R}^l \gamma$ y $\beta \xrightarrow{R}^k \gamma$. Ahora también por HI sabemos que existen δ_1, δ_2 tal que $r_1 \xrightarrow{R}^l \delta_1, r_2 \xrightarrow{R}^k \delta_2, \gamma \rightarrow_R \delta_1, \gamma \rightarrow_R \delta_2$. Finalmente, por propiedad de diamante con $\gamma, \delta_1, \delta_2$ vemos que existe s tal que $\delta_1 \rightarrow_R s, \delta_2 \rightarrow_R s$.

Uniendo todo esto tenemos que $r_1 \xrightarrow{R}^l \delta_1 \rightarrow_R s$ y $r_2 \xrightarrow{R}^k \delta_2 \rightarrow_R s$ por lo tanto $r_1 \xrightarrow{R}^{l+1} s$ y $r_2 \xrightarrow{R}^{k+1} s$ que era lo que buscábamos. Abajo hay un esquema de la demostración.



Lema 2.7.2

Sea \rightarrow_R Church-Rosser, r_1, r_2 en forma normal, y t tal que $t \xrightarrow{R}^* r_1, t \xrightarrow{R}^* r_2$ queremos probar que $r_1 = r_2$.

Como \rightarrow_R es Church-Rosser y $t \xrightarrow{R}^* r_1, t \xrightarrow{R}^* r_2$, sabemos que existe un s tal que $r_1 \xrightarrow{R}^* s$ y $r_2 \xrightarrow{R}^* s$.

Dado que r_1 está en forma normal, no existe ningún e tal que $r_1 \rightarrow_R e$, por lo que el único elemento tal que $r_1 \xrightarrow{R}^* s$ es r_1 . Por lo tanto $s = r_1$. Análogamente ocurre con r_2 , por lo tanto $r_2 = s$ y por ende $r_1 = r_2$.

Parte II: Semántica denotacional y teoría de categorías

Ejercicio 5: demostrar el siguiente teorema

Teorema 4.12

En Set, los epimorfismos son exactamente las funciones sobreyectivas (las funciones $f : A \rightarrow B$ para las cuales para cada $b \in B$ existe un $a \in A$ tal que $f(a) = b$).

\Rightarrow) Sea $A \xrightarrow{f} B$ una función sobreyectiva. Supongamos que no es un epimorfismo, por lo tanto existen $B \xrightarrow{g} C$ y $B \xrightarrow{h} C$ tales que $g \circ f = h \circ f$ pero $g \neq h$. Sea $y \in B$ tal que $g(y) \neq h(y)$ el cual existe por ser g y h distintas. Como f es sobreyectiva, existe $x \in A$ que cumple $f(x) = y$, luego $g(y) = g(f(x))$ y $h(y) = h(f(x))$ y por ende $g \circ f \neq h \circ f$, lo cual contradice las hipótesis de g y h .

\Leftarrow) Sea $A \xrightarrow{f} B$ un epimorfismo. Supongamos que no es sobreectiva, luego existe $b \in B$ tal que para todo $a \in A$, $f(a) \neq b$. Sean g y h flechas de B en C tales que

$$g(x) = x \quad h(x) = \begin{cases} c & \text{si } x = b \\ x & \text{caso contrario} \end{cases}$$

Luego, ver que $g(f(x)) = f(x)$ y $h(f(x)) = f(x)$ pues $f(x) \neq b$ para todo $x \in A$, por lo tanto $g \circ f = h \circ f$ y dado que f es un epimorfismo se tiene que $g = h$ lo cual contradice las hipótesis.

Ejercicio 10: demostrar que List es un functor

Comportamiento functorial de List

Sea $f : S \rightarrow S'$ una función entre conjuntos, probar que

1. $\text{List}(\text{Id}_S) = \text{Id}_{\text{List}(S)}$
2. $\text{List}(g \circ f) = \text{List}(g) \circ \text{List}(f)$ para toda función $g : S' \rightarrow S''$.

1. *Identidad.* Sea $L = [s_1, \dots, s_n] \in \text{List}(S)$ una lista cualquiera, luego se tiene:

$$\text{List}(\text{Id}_S)(L) = [\text{Id}_S(s_1), \dots, \text{Id}_S(s_n)] = [s_1, \dots, s_n] = \text{Id}_{\text{List}(S)}(L)$$

por lo tanto $\text{List}(\text{Id}_S) = \text{Id}_{\text{List}(S)}$.

2. *Composición.* Sean $f : S \rightarrow S'$, $g : S' \rightarrow S''$ y $L = [s_1, \dots, s_n]$ una lista en $\text{List}(S)$. Entonces:

$$\text{List}(g \circ f)(L) = [(g \circ f)(s_1), \dots, (g \circ f)(s_n)] = [g(f(s_1)), \dots, g(f(s_n))]$$

Luego, desde el otro lado

$$[g(f(s_1)), \dots, g(f(s_n))] = \text{List}(g)([f(s_1), \dots, f(s_n)]) = (\text{List}(g) \circ \text{List}(f))(L)$$

Dado que esto vale para toda lista se tiene que

$$\text{List}(g \circ f) = \text{List}(g) \circ \text{List}(f)$$

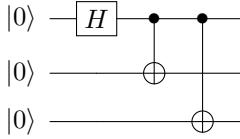
lo cual demuestra la propiedad de composición.

Por ende List cumple con las dos condiciones por lo que queda probado que es un functor.

Parte III: Computación cuántica

Ejercicio 15: dar un circuito que genere el estado $\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$ a partir de la entrada $|000\rangle$

Se propone el siguiente circuito,



Al analizar la traza se ve que, comenzando con la entrada $|000\rangle$ se obtiene el estado deseado.

$$\begin{aligned} |000\rangle &\xrightarrow{H \otimes I \otimes I} \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)|00\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |100\rangle) \\ &\xrightarrow{CNOT(1,2)} \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle) \xrightarrow{CNOT(1,3)} \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \end{aligned}$$

Ejercicio 26: probar el siguiente teorema

Teorema 8.22

Para todo operador densidad ρ se tiene $tr(\rho^2) \leq 1$. Además, la igualdad se cumple si y solo si ρ está en un estado puro.

Recordemos que para un conjunto de estados puros $\{(p_i, |\psi_i\rangle)\}$, el operador de densidad es $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Por el Teorema 8.25 del apunte se tiene que puede ser escrito como $\rho = \sum_j \lambda_j |j\rangle\langle j|$ donde los $|j\rangle$ son ortonormales y $\lambda_j \in \mathbb{R}_0^+$. Vemos entonces que:

$$tr(\rho^2) = tr\left(\left(\sum_i \lambda_i |i\rangle\langle i|\right)^2\right) = tr\left(\sum_i \sum_j \lambda_i \lambda_j |i\rangle\langle i| |j\rangle\langle j|\right) = \sum_i \sum_j \lambda_i \lambda_j tr(|i\rangle\langle i| |j\rangle\langle j|)$$

Como los vectores son ortonormales, tenemos que $\langle i|j \rangle = \delta_{ij}$, entonces:

$$\sum_i \sum_j \lambda_i \lambda_j tr(|i\rangle\langle i| |j\rangle\langle j|) = \sum_i \sum_j \delta_{ij} \lambda_i \lambda_j tr(|i\rangle\langle j|) = \sum_i \lambda_i^2 tr(|i\rangle\langle i|)$$

Luego, por el Teorema 8.12 del apunte, $tr(|i\rangle\langle i|) = \langle i|i \rangle = 1$, por lo que $tr(\rho^2) = \sum_i \lambda_i^2$. Además es sabido que:

$$tr(\rho) = tr\left(\sum_i \lambda_i |i\rangle\langle i|\right) = \sum_i \lambda_i = 1$$

Como los λ_i son positivos, se tiene que $0 \leq \lambda_i \leq 1$ para todo i , por lo tanto $\lambda_i^2 \leq \lambda_i$. Luego:

$$tr(\rho^2) = \sum_i \lambda_i^2 \leq \sum_i \lambda_i = tr(\rho) = 1$$

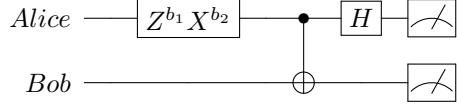
En el caso en el que ρ está en estado puro, se puede escribir como $|\psi\rangle\langle\psi|$, y es fácil ver que $tr(\rho^2) = tr(|\psi\rangle\langle\psi|\psi\rangle\langle\psi|) = tr(|\psi\rangle\langle\psi|) = \langle\psi|\psi\rangle = 1$.

Cuando ρ es un estado mixto, no puede ser escrito de esa forma, por lo que por lo menos dos λ_i son no nulos, esto junto con que $\sum_i \lambda_i = 1$ y $0 \leq \lambda_i \leq 1$, fuerza a que $\lambda_i < 1$ para todo i . Por lo tanto $\lambda_i^2 < \lambda_i$ y entonces

$$tr(\rho^2) = \sum_i \lambda_i^2 < \sum_i \lambda_i = 1$$

Algoritmo

El algoritmo de codificación superdensa empieza en un estado β_{00} , donde Alice tiene el primer qubit y Bob el segundo. Luego de aplicar la primer compuerta, Alice envía su qubit a Bob. Alice quiere enviar los bits $b_1 b_2$ clásicos a Bob, el circuito es de la forma:



Caso $b_1 = 0, b_2 = 0$.

$$\begin{aligned}\beta_{00} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &\xrightarrow{X^0 \otimes I} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &\xrightarrow{Z^0 \otimes I} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &\xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |0\rangle = |+\rangle \otimes |0\rangle \\ &\xrightarrow{H \otimes I} |0\rangle \otimes |0\rangle = |00\rangle\end{aligned}$$

Caso $b_1 = 0, b_2 = 1$.

$$\begin{aligned}\beta_{00} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &\xrightarrow{X^1 \otimes I} \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\ &\xrightarrow{Z^0 \otimes I} \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\ &\xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) \\ &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |1\rangle = |+\rangle \otimes |1\rangle \\ &\xrightarrow{H \otimes I} |0\rangle \otimes |1\rangle = |01\rangle\end{aligned}$$

Caso $b_1 = 1, b_2 = 0$.

$$\begin{aligned}\beta_{00} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &\xrightarrow{X^0 \otimes I} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &\xrightarrow{Z^1 \otimes I} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ &\xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \\ &= \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes |0\rangle = |- \rangle \otimes |0\rangle \\ &\xrightarrow{H \otimes I} |1\rangle \otimes |0\rangle = |10\rangle\end{aligned}$$

Caso $b_1 = 1, b_2 = 1$.

$$\begin{aligned}\beta_{00} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &\xrightarrow{X^1 \otimes I} \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\ &\xrightarrow{Z^1 \otimes I} \frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle) \\ &\xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(-|11\rangle + |01\rangle) \\ &= \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes |1\rangle = |- \rangle \otimes |1\rangle \\ &\xrightarrow{H \otimes I} |1\rangle \otimes |1\rangle = |11\rangle\end{aligned}$$

Lambda cálculo cuántico a control clásico

El término que implementa el algoritmo en el lambda cuántico a control clásico es el siguiente:

```
(λb1.λb2.
  let ⟨q1, q2⟩ = EPR★
  in let ⟨a, b⟩ = CNOT(
    let ⟨x1, x2⟩ = if b2 then ⟨Xq1, q2⟩ else ⟨q1, q2⟩
    in if b1 then ⟨Zx1, x2⟩ else ⟨x1, x2⟩)
  in ⟨meas (Ha), meas b⟩)
```

donde $EPR = \lambda x.CNOT\langle H(\text{new } 0), \text{new } 0 \rangle$

El tipo del término es $[\![\cdot]\!], t : !bit \multimap !bit \multimap qubit \otimes qubit$

Veamos su reducción paso a paso cuando es ejecutado con $b_1 = b_2 = 1$.